DETAILED ACTION

1. Examiner initiated interview has been made to amend independent claim 73 and dependent claims depending on claim 73 to correct 101 statutory problem that was resolved by the agreement on the telephone interview with Lori A. Gordon on July 2, 2008.

2. Terminal disclaimer filed on 03/06/2007 to disclaim 09/892,242 and accepted by the office.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Lori A. Gordon on July 2, 2008.

3. Claims 73, 51-54, 74-77, and 48-49 are amended as follows:

73. (Currently Amended) An integrated circuit [[layout]] associated with a cryptography engine for performing cryptographic operations on a data block having a first portion and a second portion, the integrated circuit [[layout]] comprising:

a key scheduler configured to provide a plurality of keys for cryptographic operation rounds, wherein the key scheduler includes a multi-stage pipeline and is further

configured to generate a round key each clock cycle after a series of initialization clock cycles; and

cryptographic round logic, wherein the cryptographic round logic is configured to receive a key from the key scheduler for a current cryptographic round and wherein the cryptographic round logic includes:

means for combining via a first logical operation the key provided by the key scheduler with a first bit sequence to generate a second bit sequence, wherein the first bit sequence is an expansion of the first portion of the data block;

substitution logic for receiving the second bit sequence and for generating a third bit sequence;

a first inverse permutation logic for performing, during an initial cryptographic round, an inverse permutation of the first portion of the data block and for generating a first inverse permuted bit sequence, wherein the first inverse permuted bit sequence is a first input bit sequence for a subsequent cryptographic round;

a second inverse permutation logic for performing, during an initial cryptographic round, an inverse permutation of the second portion of the data block and for generating a second inverse permuted bit sequence;

means for combining via a second logical operation the third bit sequence with the second inverse permuted bit sequence to generate a fourth bit sequence; and

a permutation logic for permuting the fourth bit sequence and generating a permuted bit sequence, wherein the permuted bit sequence is a second input bit sequence for the subsequent cryptographic round.

51. (Currently Amended) The integrated circuit [[layout]] of claim 73, wherein the key scheduler comprises a determination stage, a shift stage, a propagation stage, and a consumption stage.

52. (Currently Amended) The integrated circuit [[layout]] of claim 51, wherein a first shift amount for a first key is identified in the determination stage using a first round counter value.

53. (Currently Amended) The integrated circuit [[layout]] of claim 73, further comprising a multiplexer circuitry including a two-level multiplexer.

54. (Currently Amended) The integrated circuit [[layout]] of claim 53, wherein the two-level multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to an output stage of the multiplexer.

74. (Currently Amended) The integrated circuit [[layout]] of claim 73, wherein the first and second logical operations are binary XOR operations.

75. (Currently Amended) The integrated circuit [[layout]] of claim 73, wherein the first bit sequence is a bit sequence expanded by an expansion logic.

76. (Currently Amended) The integrated circuit [[layout]] of claim 73, wherein the second bit sequence is less than the first bit sequence.

77. (Currently Amended) The integrated circuit [[layout]] of claim 73, wherein the data block contains bits 0 to M, the first portion contains bits 0 to N, and the second portion contains bits N+I to M.

48. (Currently Amended) The integrated circuit [[layout]] of claim 76, wherein the first bit sequence is four bits.

49. (Currently Amended) The integrated circuit [[layout]] of claim 48, wherein the expanded first bit sequence is less than six bits.

Response to Arguments

4. Applicant's arguments on 04/03/2008 are persuasive.

Allowable Subject Matter

5. Claims 5-8, 11-14, 17-21, 48-49, 51-54, and 68-79 are allowed.

The following is an examiner's statement of reasons for allowance:

Prior arts of record neither alone nor in combination teach a cryptography engine comprising cryptographic round logic, wherein the cryptographic round logic is configured to receive a key from the key scheduler for a current cryptographic round and wherein the cryptographic round logic includes: means for combining via a first logical operation the key provided by the key scheduler with a first bit sequence to generate a second bit sequence, wherein the first bit sequence is an expansion of the first portion of the data block; substitution logic for receiving the second bit sequence and for generating a third bit sequence; a first inverse permutation logic for performing, during an initial cryptographic round, an inverse permutation of the first portion of the data block and

for generating a first inverse permuted bit sequence, wherein the first inverse permuted bit sequence is a first input bit sequence for a subsequent cryptographic round; a second inverse permutation logic for performing, during an initial cryptographic round, an inverse permutation of the second portion of the data block and for generating a second inverse permuted bit sequence; means for combining via a second logic operation the third bit sequence with the second inverse permuted bit sequence to generate a fourth bit sequence; and a permutation logic for permuting the fourth bit sequence and generating a permuted bit sequence, wherein the permuted bit sequence is a second input bit sequence for the subsequent cryptographic round.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Eleni A Shiferaw/

Primary Examiner, Art Unit 2136

July 2, 2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136